

STANDARD NETWORKING FORMS

Throughout this book you have learned about various operating procedures and policies that help your IT operations, upgrades, and installations run more smoothly. This appendix offers examples of forms you can use when planning and maintaining a network. Recognize that you may need to change the forms slightly to suit your environment. However, having a form template can help you remember steps you may otherwise have forgotten.

This appendix provides the following forms:

- Server Installation Checklist – Windows 2000
- Server Installation Checklist – NetWare
- Server Installation Checklist – RedHat Linux
- User Account Creation Form
- Technical Support Contacts Form
- Incident Report Form
- Network Security Checklist

Server Installation Checklist – Windows 2000

Installer: _____ Date: _____

Model and Serial Number: _____

RAM: _____ Processor: _____ Hard Disk: _____

Server is a: Domain Controller Member Server

Server Name: _____

Domain Name: _____

NIC 1 Type: _____ IRQ: _____ Base I/O: _____ DMA: _____

NIC 2 Type: _____ IRQ: _____ Base I/O: _____ DMA: _____

Protocols:

NetBEUI

TCP/IP

NWLink IPS/SPX-Compatible Protocol

IP Address: _____

Other: _____

Gateway: _____

DNS Server: _____

Disk Controller Type(s): _____

Partitions:

1: Type: _____ Size: _____ Name: _____

2: Type: _____ Size: _____ Name: _____

3: Type: _____ Size: _____ Name: _____

4: Type: _____ Size: _____ Name: _____

Registration Key: _____

Licensing Mode: Per Server Per Seat

Server Installation Checklist – NetWare

Installer: _____ Date: _____

Model and Serial Number: _____

RAM: _____ Processor: _____ Hard Disk: _____

Server Name: _____

Disk Controller Types(s): _____

NIC 1 Type: _____ IRQ: _____ Base I/O: _____ DMA: _____

NIC 2 Type: _____ IRQ: _____ Base I/O: _____ DMA: _____

Partitions:

1: Type: _____ Size: _____ Name: _____

2: Type: _____ Size: _____ Name: _____

3: Type: _____ Size: _____ Name: _____

4: Type: _____ Size: _____ Name: _____

NDS Tree: _____ NDS Container: _____

Licensing Number: _____

Protocols:

 NetBEUI TCP/IP NWLink IPX/SPX Compatible Protocol

IP Address: _____

 Other: _____

Gateway: _____

DNS Server: _____

Server Installation Checklist – RedHat Linux

Installer: _____ Date: _____

Model and Serial Number: _____

RAM: _____ Processor: _____ Hard Disk: _____

Keyboard Type: _____ Monitor: _____

Packages to Install: _____

Mouse Type: _____

Video Card Type: _____

TCP/IP Settings:

IP Address: _____

Netmask: _____

Default Gateway: _____

Primary Nameserver: _____

Domain Name: _____

Hostname: _____

User Account Creation Form

User Name: _____

Department/Location: _____ Phone: _____

Date Created: _____ By: _____

Requested By: _____

Approved By: _____

User ID: _____

Context (NetWare) or Domain (Windows 2000): _____

Group Memberships: _____

Home Directory: _____

Password Restrictions:

 Minimum password length: _____ Require unique passwords? Yes No

 Days before password expires: _____ Grace logins: _____

Login Restrictions:

 Valid login times: _____ Maximum connections: _____

 Address restrictions: _____ Location restrictions: _____

Technical Support Contacts Form

Vendor Name: _____

Address: _____

General Phone Number: _____ Tech. Support Phone Number: _____

General Web Page: _____ Tech. Support Web Page: _____

Contact Name: _____

Products Supported:

Product Name: _____ Product License Number: _____

Support Agreement Specifies:

Support Experiences with Vendor:

Date: Reason for call: Resolution:

Incident Report Form**D**

User Name: _____

User ID: _____

Location: _____ Phone: _____

Date: _____ Time: _____

Received By: _____

Nature of the problem:

Resolution:

Date: _____ By: _____

Notes:

Follow-up Call:

Date: _____ By: _____

Notes:

Network Security Checklist

- Write and enforce security policy
- Communicate security policy to all employees
- Identify vulnerabilities
- Enforce use of passwords
- Require minimum password length
- Require frequent password changes
- Disable Administrator user on servers (use another ID with equivalent privileges)
- Implement virus scanning on servers and workstations
- Implement firewalls between private and public networks
- Restrict logins to TCP/IP ports
- Properly configure firewall and router access
- Review remote access links for security threats
- Implement enterprise-wide intrusion detection
- Encrypt sensitive data in transit (for example, use digital certificates)
- Implement automated, enterprise-wide virus detection
- Implement badge access for equipment and telecommunications rooms
- Use security cameras to monitor entrances and equipment rooms
- Perform background checks on prospective employees
- Plan for security breaches by having a trained response team